Abstract

Due to the rising number of attacks on software hosted in the cloud, new innovative technologies for providing security guarantees to the hosting parties need to be developed. In order to improve upon the lack of such technology, three new concepts for runtime attestation of an user access management system, called user access engine, inside of trusted execution environments are developed and analyzed. All three concepts provide fundamental security for systems by allowing a detached attestation server to detect malicious actions on the system after they occurred during runtime. These concepts include the generation of a hash chain structure, the new combination of trusted execution environments with virtual trusted platform modules and the utilization of existing decentralized user rights management via JSON web tokens for user authentication.

All proposed and played through critical attacks could be averted within the boundaries set by the research project. Only attackers with a substantial amount of resources, along with physical access to the hosting platform's hardware can utilize previously known hardware attacks against the platform, independently of the proposed concepts. These attacks were out of scope for this work. For all other attack scenarios, this thesis advances the concept of runtime analysis by an important margin into the realm of future real world applications, utilizing not only the base applications running in the cloud, but also user management systems. This is a novel approach for an attestation scheme of a web service architecture.